McAfee ePolicy Orchestrator 4.5 Reporting Guide

McAfee®

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Introducing ePolicy Orchestrator 4.5 Reporting **4**

Using this guide 4

Finding documentation for McAfee enterprise products 5

Using Preconfigured Queries **6**

About query groups 6

Working with preconfigured queries 7

Creating Custom Queries and Reports **10**

Creating a Managed Systems query 10

Converting the VSE DAT versions query to a pie chart 11

Creating a Boolean Pie Chart to display compliance 12

Creating a dashboard monitor to display VirusScan Enterprise DAT compliance 14

Exporting query results to create a PDF report 14

Appendix: Permission Sets and Query Variables **16**

Permission set details 16

Managed Systems properties 17

Computer properties 18

Applied Policies properties 18

Detected Systems properties 19

Common product properties 20

Common Events Format 20

Introducing ePolicy Orchestrator 4.5 Reporting

McAfee ePolicy Orchestrator 4.5 provides a scalable platform for centralized policy management and enforcement of your security products and the systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

This document provides information about ePolicy Orchestrator 4.5 reporting functionality using the built-in query system. This system can simplify the process of extracting important information you need to manage your network.

Contents

- Using this guide
- Finding documentation for McAfee enterprise products

Using this guide

ePolicy Orchestrator 4.5 is delivered with a built-in query system. This includes the Query Builder wizard, a tool you can use to create custom queries, which result in informative user-configured charts and tables that contain user-specified data. This guide provides some examples and scenarios you can use to become more familiar with the query and reporting system. It includes content based on the following assumptions:

- You have access to an ePolicy Orchestrator 4.5 server with Global Administrator privileges, or you have been assigned the appropriate permission sets to access the functionality used by the scenarios that follow. For more information on permission sets, see *Permission set details* in the *Permission Sets and Query Variables* chapter.
- Your environment includes at least one system with a McAfee Agent deployed (agent version 4.0 or later).
- Your environment includes at least one system with McAfee VirusScan® Enterprise deployed (version 8.5i or later).
- You have at least one VirusScan Enterprise DAT installed on your managed systems.

NOTE: An environment with multiple systems provides more robust results.

Audience

This information is intended primarily for network administrators who are responsible for their company's security program, and assumes the customer has installed and used ePolicy Orchestrator in a lab environment. Users other than your Global Administrator might be assigned to run, edit, and create queries, but those users must be given permission by their network administrator. See *Permission set details* in the *Permission Sets and Query Variables* chapter.

Finding documentation for McAfee enterprise products

To access the documentation for your McAfee products, use the McAfee ServicePortal.

1. Go to the McAfee ServicePortal (http://mysupport.mcafee.com) and, under **Self Service**, click **Read Product Documentation**.
2. Select a **Product**.
3. Select a **Version**.
4. Select a product document

Product documentation by phase

McAfee documentation provides the information you need during each phase of product implementation, from installing a new product to maintaining existing ones. Depending on the product, additional documents might also be available. After a product is released, information regarding the product is entered into the online KnowledgeBase, available through the McAfee ServicePortal.

Installation phase — Before, during, and after installation

- *Release Notes*
- *Installation Guide*

Setup phase — Using the product

- *Product Guide*
- *Online Help*

Maintenance phase — Maintaining the software

- *KnowledgeBase* (http://mysupport.mcafee.com)

Using Preconfigured Queries

ePolicy Orchestrator includes preconfigured queries you can use to report on and manage your network. This chapter describes the processes used to run and modify preconfigured queries so that you can generate reports about your ePolicy Orchestrator server, including the following types of information:

- Managed products deployed throughout your network. For example, the McAfee Agent or McAfee VirusScan Enterprise.
- User actions on your ePO server. For example, how many failed login attempts have occurred on your server in the last 30 days.
- Policy assignment. For example, which policies are assigned to each system in your network.

The preconfigured queries available to you depend on which managed products you have installed. They use a variety of chart types to display query results, and can be modified to suit your needs.

TIP: McAfee recommends that you create a duplicate of a preconfigured query before modifying it, so you can retain the original functionality of each query. For more information on duplicating queries, see *Customizing preconfigured queries*.

Contents

- About query groups
- Working with preconfigured queries

About query groups

There are two pre-defined query groups in ePolicy Orchestrator, which contain all queries:

- My Groups
- Shared Groups

The queries in these groups are further organized into subgroups. All preconfigured queries appear in the **Shared Groups** category on the **Queries** page.

NOTE: When upgrading from an earlier version of ePolicy Orchestrator, queries might appear in different categories if you have modified their organization.

By default, queries in the **Shared Groups** category are accessible to any user with the appropriate permissions. Users without the appropriate permissions can see the query, but are not able to run the query. For example, if a user has full permissions to use queries, but has no permissions for VirusScan Enterprise, the user cannot run any VirusScan Enterprise queries.

All preconfigured queries are included in the **Shared Groups** category. Preconfigured queries that appear in the **Shared Groups** category by default are organized into subgroups by functionality and managed product dependencies.

Queries in the **My Groups** category are available only to the user who creates them, the query owner.

When creating or modifying a query, you can choose the group in which it is saved:

- Private group. These queries reside in a user-configured subgroup of the **My Groups** category and can only be viewed by the owner.
- Public group. These queries reside in **Shared Groups** category and can be accessed by any user with query permissions.

Working with preconfigured queries

Use these tasks to familiarize yourself with preconfigured queries. Each task builds upon the previous one. When you have completed them all, you should be able do the following:

- Run queries
- Duplicate queries
- Edit queries

Tasks

▸ Running preconfigured queries
▸ Customizing preconfigured queries

Running preconfigured queries

Use this task to run the preconfigured User Auditing query, **Failed User Actions in ePO Console within Last 30 days**, and interact with the results. When completed successfully, this task returns a table that provides details about all failed user actions that have occurred within the ePO console in the last 30 days. Tables such as this are the base form of all query results.

Task

For option definitions, click **?** in the interface.

1. In the ePO console, click **Menu | Queries** to open the Queries page.
2. Locate the **Failed User Actions in ePO Console within Last 30 days** using one of the following methods:
   - In the **Groups** column, click **Shared Groups | User Auditing**.
   - Type the name of the query into the **Quick find** field and click **Apply**.

     TIP: You can type a partial name to narrow the results.

   - Use the scroll bar to locate the query. Queries are arranged alphabetically.
3. Click **Run** in the **Actions** column to the right of the query. The query results are displayed in a table titled with the name of the query, **Failed user Actions in ePO Console within Last 30 days**.

   NOTE: You can also click the checkbox next to the query and click **Actions | Run** to run queries.

4 Click any row entry in the table to view more details about that system. The **Audit Log Entry Details** page opens.

5 Click **Close** to return to the query results table, then click **Close** again to return to the **Queries** page.

6 In the **Actions** column, click **Details** to review the details of this query.

Customizing preconfigured queries

Use this task to customize the preconfigured query, **Failed User Actions in ePO Console within Last 30 Days**. When completed successfully, this task creates a custom query that reports on the successful user actions that have occurred in the ePO console in the last 30 days, in the form of a pie chart.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Queries** and create a new private query group:

   a Click **Group Actions | New Group**.

   b **Name** the new group **Custom Queries** and choose **Private group (My Groups)** from the **Group visibility** options.

   c Click **Save**. The Queries page opens.

   d In the **Groups** column, expand the **My Groups** list to view your Custom Queries subgroup.

2 In the **Quick find** field, type Failed User Actions in ePO Console within Last 30 Days and click **Apply**.

3 Click the checkbox next to the query, then click **Actions | Duplicate**. The Duplicate dialog box opens.

4 In the **New Name** field, type **Successful User Actions in ePO Console within Last 30 Days**.

5 From the **Group to receive** menu, select **Custom Queries** under the **My Groups** category. The duplicated query appears in the **My Groups | Custom Queries** subgroup.

6 In the **Actions** column next to your custom query, click **Edit**. The Query Wizard opens.

7 Click **Next** to advance to the Columns page. From the **Available Columns** list, add the **Success** column.

8 Reorder the columns so that **Success** is the first column in the table.

   NOTE: To reorder columns, use the left and right arrows, or use drag-and-drop to move the desired column into a new position.

9 Click **Next** to open the Filter page. Set the **Success** value to **True**, then click **Run**. This query now returns all successful user actions performed in the last 30 days.

10 Click **Edit Query** to return to the Query Wizard.

11 Change the chart type to **Pie Chart** and modify the configuration to match the following values:

Option	Value
Labels are	**User Name**
Sort by	**Value (Descending)**

Option	Value
Pie slice values are	**Number of** and **Action** NOTE: Click the **Show Total** checkbox.

12 Click **Run**. The query results now show how many successful actions each user has performed in the last 30 days. You can click any wedge in the pie, or row entry in the summary table, to view the details about each user's actions.

13 Click **Save** and:

a Name the query **Successful User Actions by User - Pie**.

b Provide a meaningful description of the query in the **Notes** field.

c Click **Save**.

Creating Custom Queries and Reports

The tasks in this scenario illustrate how the ePolicy Orchestrator query and reporting feature helps you manage your environment.

Ensuring that the most current VirusScan Enterprise DATs are installed is an essential part of managing security threats. Using ePolicy Orchestrator to report on DAT compliance can simplify this important task.

Complete the tasks in the Contents list sequentially to:

- Create a **Managed Systems** query that returns a table containing the **System Name**, **Last Communication**, and **DAT Version (VirusScan Enterprise)** installed for every managed system in your network.
- Convert the **Managed Systems** table to a pie chart to create a graphic representation of the information.
- Convert the **Managed Systems** pie chart to a Boolean pie chart that displays the same information displayed as a compliance chart.
- Create a dashboard monitor from the compliance chart to view the DAT compliance of managed systems "at-a-glance."
- Export the DAT compliance information to a PDF report for distribution to stakeholders in your organization.

Contents

- Creating a Managed Systems query
- Converting the VSE DAT versions query to a pie chart
- Creating a Boolean Pie Chart to display compliance
- Creating a dashboard monitor to display VirusScan Enterprise DAT compliance
- Exporting query results to create a PDF report

Creating a Managed Systems query

This task creates a new Managed Systems query that reports the VirusScan Enterprise DAT versions that are deployed to managed systems in your network.

Task

For option definitions, click **?** in the interface.

1. Click **Menu | Reporting | Queries**, then click **Actions | New Query**. The **Query Wizard** opens.
2. In the **Feature Group** pane, click **System Management**. Then in the **Result Types** pane, click **Managed Systems** and click **Next**.

3 In the **Display Results As** pane, click **Table**, then click **Next**.

4 In the **Available Columns** pane, select the following columns to include in the table, then click **Next**:

Available columns by property category	Add this column
Managed Systems	**Last Communication** (included by default) NOTE: Although this information is not critical to the overall scenario, the last communication time can be useful when considering why a system has a particular DAT version installed. For example, if a system has not communicated in 4 days, you would not expect the DAT you pushed out yesterday to be installed. **System Name** (included by default)
VirusScan Enterprise	**DAT Version**

5 In the **Filter** page, make sure no **Available Properties** are selected, then click **Run**. A table containing all the systems in your network is created.

NOTE: You can view more details about any system by clicking its row entry in the table, which opens the **System Details** page.

6 Click **Save** and specify the following query details:

Details	Value
Name	VSE DAT versions.
Notes	This table displays the VirusScan Enterprise DAT versions that are deployed to systems in the network.
Group	Create a new, private group titled VSE Compliance.

7 Click **Save**. The **Query** page opens.

8 View the details of this query:

a In the **Query** page, click **My Groups | VSE Compliance**.

9 In the **Actions** column, click Details.

Converting the VSE DAT versions query to a pie chart

In the previous task you created a table based query titled **VSE DAT versions**. If you have a large number of managed systems in your network, the table format is not the best method to extrapolate meaningful data. Use this task to create a more visually accessible representation of this data.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Reporting | Queries**, then in the **Groups** pane, click **My Groups | VSE Compliance**.

2 In the **Queries** pane, click the checkbox next to the **VSE DAT versions** query, then click **Actions | Duplicate**.

TIP: McAfee recommends that you duplicate a query and edit the copy, rather than modifying the original, to ensure you retain functionality of the existing query.

3 In the **Duplicate** dialog box, type VSE DAT versions - pie chart as the **New Name** for the query. Leave **Group to receive copy** set to **VSE Compliance**, then click **OK**.

4 In the **Actions** column next to the new query, click **Edit**. The **Query Wizard** opens to the **Chart** page.

5 Click **Pie Chart** and specify the following options:

Option	Value
Labels are	**DAT Version (VirusScan Enterprise)**
Sort by	**Value (Descending)**
Show "other"	Checkbox selected
Pie slice values are	**Number of Managed Systems**
Show Percentage	Checkbox selected

6 Click **Run** to display the updated query results, then click **Save**. Type VSE DAT by managed systems as the name for this query, and save it to the VSE Compliance group.
You can use this query to view which VirusScan Enterprise DAT versions are currently deployed to your managed systems.

Creating a Boolean Pie Chart to display compliance

In the previous task, you converted your table based query to a pie chart that groups systems together based on which DAT versions are installed on the managed systems in your network. Use this task to modify that pie chart so it dislpays VSE DAT compliance. When completed successfully, the query results will display a pie chart showing two categories:

- Compliant Managed Systems — the green portion of the Pie Chart. These are systems that have the latest VirusScan Enterprise DAT installed.
- Non-compliant Managed Systems — the red portion of the Pie Chart. These are managed systems that do not the latest VirusScan Enterprise DAT installed.

Before you begin

It is helpful, when completing this task, to know the version number of the most current DAT available from McAfee.

1 Click **Menu | Reporting | Dashboards**, then click the **ePO Summary for 4.5** tab to display the summary dashboard.

2 Look in the **MyAvert Threat Advisory** monitor for the **Latest Available DAT** version.

Figure 1: MyAvert Threat Advisory monitor

NOTE: For this task, it is not necessary to have the latest available DAT checked into your repository.

Task

For option definitions, click **?** in the interface.

1 **Duplicate** the **VSE DAT by managed systems** pie chart query.

2 **Edit** the new query, and select **Boolean Pie Chart** from the **Display Results As** pane, then set the following options:

Option	Value
Criteria to match	1 Click **Configure Criteria**. 2 In the **Configure Criteria** page select **DAT Version (VirusScan Enterprise)** from the **VirusScan Enterprise Properties** in the **Available Properties** pane. 3 Set the **Comparison** property to **Greater than or equals**. 4 Set the **Value** to the latest available DAT. For example, in the image above the latest available DAT is 5786.0000. 5 Click **OK**. The **Chart** page of the **Query Wizard** opens again.

Option	Value
Show Criteria in Chart	Checkbox selected
Label for matching slice	**Compliant**
Label for non-matching slice	**Non-Compliant**
Pie slice values are	**Number of Managed Systems**
Show Total	Checkbox selected

3 Click **Run** to view the results.

4 Click **Save**, then in the **Name** field, type VSE DAT Compliance.

Creating a dashboard monitor to display VirusScan Enterprise DAT compliance

Use this task to create a dashboard monitor from the Boolean pie chart query you created in the previous task. Creating a dashboard monitor enables you to view the DAT compliance of your managed systems "at-a-glance."

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Dashboards**, then click **Options | Manage Dashboards**.

2 In the **Dashboards** pane, click **New Dashboard**. Type VSE DAT compliance in the **Name** field in the **New Dashboard** page.

3 From the **Size** menu, select **2x1 Layout**.

4 Click **New Monitor**, then in the **Select Monitor** dialog box choose **Queries** from the **Category** menu.

5 In the **Monitor** menu, select **My Groups - VSE Compliance | VSE DAT compliance**, then click **OK** and **Save**.

6 When the **Make Active** dialog box opens, click **Yes**, then click **Close**.

7 On the **Dashboards** page, click **New Dashboard** on the tab bar to view your VSE DAT compliance pie chart.

NOTE: You can click any pie slice to view details about that group. To gather details about an individual system, click any row entry in the table that appears.

Exporting query results to create a PDF report

Use this task to create a PDF report from the **VSE DAT compliance** query you created in the previous tasks.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Queries**, then run the **VSE DAT compliance** query.

2 Click **Options | Export Data**, then specify the following options for your report:

Option	Value
What to export	**Chart data only**
File format	**PDF** NOTE: You can optionally choose **Show filter criteria** and **Include a cover page with this text** to provide important details about the query results.
Show filter criteria	Check this box
What to do with exported files	Open or save from a link

NOTE: To generate a report that includes drill-down tables, you must use the HTML file format. If you choose this output format with the intention of distributing the report, you must select the option to zip the output files, because more than one file is created for the report.

3 Click **Export**.

4 Right-click the **VSE_DAT_compliance.pdf** link and save the file.

5 Open the file to review the PDF report.

Appendix: Permission Sets and Query Variables

This chapter contains details about Permission Sets and many of the variables you can use when creating queries and reports. Use the tables included as a reference when working with queries.

Contents

- Permission set details
- Managed Systems properties
- Computer properties
- Applied Policies properties
- Detected Systems properties
- Common product properties
- Common Events Format

Permission set details

This section provides details about the permission sets global administrators can assign. The administrators can assign existing permission sets when they:

- Create or edit user accounts
- Create or edit permission sets

When multiple permission sets are applied to a user account, they aggregate. For example, if multiple permission sets are applied to the same user account, shown in the following table, that user account has complete access to ServerXYZ.

User Account	Permission Set	ServerXYZ access
Net_Reviewer	NoAccessToXYZ	No Permission
Net_Reviewer	AllAccessToXYZ	All

NOTE: Permission sets only grant rights and access — no permission ever removes rights or access.

Default Permission sets

ePolicy Orchestrator 4.5 ships with five default permission sets that provide permissions to ePolicy Orchestrator functionality shown in the following table.

NOTE: Global Administrators do not need any additional permission sets configured to access any configuration, queries, and automatic response.

Permission Set	Permissions	Product or feature
Global administrator	All	All products and features
Executive Reviewer	View	Dashboards, events, contacts, and information that relates to the entire System Tree
Global Reviewer	View	Globally across functionality, products, and the System Tree, except for extensions, multi-server roll-up data, registered servers, and software
Group Admin	View and change	ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.
Group Reviewer	View	ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.

For additional information, see the *Working with permission sets* section in the *McAfee ePolicy Orchestrator 4.5 Product Guide*.

Managed Systems properties

Use this page to determine what managed systems properties to select when configuring queries.

The managed systems properties described in this section are used, for example, when configuring the available columns to appear when creating a query.

Table 1: Managed Systems properties

Managed Systems properties	Description
Agent GUID	Specifies the unique Agent GUID (Globally Unique Identifier) assigned to the agent deployed to a managed system.
Agent Version (deprecated)	Specifies the version number of the agent deployed to a managed system.
Communication Type	Specifies the method used by the managed system to communicate. For example, HTTPS or HTTP.
Excluded Tags	Specifies any tags that have been excluded from this system.
Installed Products	Specifies the managed products on the system.
Last Communication	Specifies the date and time the last time this system called in to the server.
Last Sequence Error	Specifies the time of the last sequence error.
Managed State	Specifies if the system is managed by ePolicy Orchestrator.
Operating System	Specifies the name of the operating system running on the system.
Sequence Errors	Specifies the time between managed system sequence errors.
Server Key	Specifies the value of the server key to query.
System Name	Specifies the NETBIOS name of the system.
System Tree Sorting	Specifies whether the system is enabled or disabled for System Tree sorting.
Tags	Specifies any tags applied to this system.
To be Transferred	Specifies if the system is to be transferred or not.

Computer properties

Computer properties provide details about the managed systems in your environment.

The computer properties described in this section are used, for example, when configuring the available columns to appear when creating a query.

Computer properties

Computer properties	Description
Agent	Specifies the version, language, and hotfix or patch version.
Agent Version	Specifies the version of the installed McAfee Agent.
Custom 1 through 4	These are the four entries per system in the ePO database which you can use for your own purposes.
Description	Specifies the user-configured description (with Edit Description) of the system in ePolicy Orchestrator.
Domain Name	Specifies the domain on the network that contains the system.
Installed Products	Specifies the managed products on the system
IP Address	Specifies the network IP address of the system.
Is 64 bit OS	Specifies if the operating system on the system is 64-bit.
Last Communication	Specifies the date and time the last time this system called in to the server.
Managed State	Specifies if the system is managed by ePolicy Orchestrator.
Operating System	Specifies the name of the operating system running on the system.
Product Coverage Reports	Specifies the version of product coverage reports, when applicable.
System Name	Specifies the NETBIOS name of the system.
System Description	Specifies any additional information about the system.
System Location	Specifies the path to the group in the System Tree that contains the system.
System Tree Sorting	Specifies whether the system is enabled or disabled for System Tree sorting.
Tags	Specifies all tags currently applied to the system.
User Name	Specifies the user name logged on to the system at the time of the last update.
VirusScan Enterprise	Specifies the details of the VirusScan software on the system such as version, language, hotfix or patch version, DAT version, and engine version.

Applied Policies properties

Use this page to determine what Applied Policy properties to select when configuring queries.

The applied policies described in this section are used, for example, when configuring the labels to appear in chart type queries.

Applied Policies properties

Applied Policies properties	Description
Assigned User Name	Displays the assigned user name to search for when configuring a query.

Applied Policies properties	Description
Computer Name	Displays the computer name of the system when configuring groups and labels during chart configuration.
Edit Status	Displays the edit status to search for when configuring a query.
Policy	Displays the policy assigned to search for when configuring a query.
Policy is Up-To-Date	Displays the up-to-date status to search for when configuring a query.
Policy Notes	Displays the notes assigned to the policy when configuring a query.
Source Server	Displays the source server name to search for when configuring a query.

Detected Systems properties

Use this page to determine which Detected Systems properties to select when configuring queries for Rogue Systems.

The Detected Systems properties described in this section are used, for example, when configuring the available columns to appear when creating a query.

Detected Systems properties

Detected Systems properties	Description
Agent Version	Specifies the version of the agent deployed to the system.
Canonical Name	Displays the friendly name of the system.
Comments	Displays user comments about the system.
Computer Name	Specifies the name of the system.
Detection Source	Specifies the source of the last detection of the system, such as Broadcast or DHCP.
Device Type	Specifies the type of detected device to use in the query. For example, computer, printer, router, or unknown.
DNS Name	Specifies the domain name of the system.
Domain	Specifies the domain the system is on.
ePO Server Name	Specifies the name of the ePO server that manages this detected system.
Exception	Specifies whether the system is marked as an exception.
Exception Category	Specifies which exception category this system belongs to.
Inactive	Specifies systems listed in the ePO database that have not been detected by a detection source in a specified time, which exceeds the period specified in the Rogue category.
Is New Detection	Specifies whether this system is a new detection.
Last Agent Communication	Specifies the date and time of the last communication from the agent deployed to the system.
Last Detected IP Address	Specifies the last detected IP address of the system.
Last Detected MAC Address	Specifies the last detected MAC address of the system.
Last Detected Organization Name	Specifies the organization name of the system at its last detection, for example, Dell.

Detected Systems properties	Description
Last Detected Time	Specifies the date and time of the last detection of the system.
Managed	Specifies systems have an active McAfee Agent that has communicated with the ePO server in a specified time.
NetBIOS Comment	Specifies the NetBIOS comment for the detected system, if any.
OS Family	Specifies the family of the operating system.
OS Platform	Specifies the operating system installed on the system.
OS Version	Specifies the version number of the operating system installed on the system.
Rogue	Specifies any systems that access your network but are not managed by your ePO server.
Rogue Action	Specifies the action being performed on a rogue system, for example, Agent Push in Progress.
Rogue State	Specifies the rogue state of a detected system, for example, Inactive Agent.
Users	Specifies the users currently associated with the system as defined by the NetBIOS call, which is typically the currently logged-on user.

Common product properties

Many McAfee managed products use some, or all, of the common product properties listed in the table below. Include these properties when building queries in order to report on important information for a specific product. For example, VirusScan Enterprise.

Common product properties

Common product properties	Description
Hotfix/patch Version	Displays the hotfix or patch properties of, for example, VSE, HIPs, Agents, and more.
Language	Displays the language properties of, for example, VSE, HIPs, Agents, and more.
Product Version	Displays the product version of, for example, VSE, HIPs, Agents, and more.
DAT Version	Displays the DAT version properties of, for example, VSE, HIPs, Agents, and more.
Engine Version	Displays the engine version properties of, for example, VSE, HIPs, Agents, and more.

Common Events Format

The Common Events Format (CEF) is used by ePolicy Orchestrator and McAfee managed products to inform and retrieve information in ePO database tables. Not all products use this format. However, understanding these fields and their purpose can aid in creating queries to report on specific information stored in your database. Threat Events are one example of how this information is reported by ePolicy Orchestrator.

CEF Fields

Field	Attributes	Purpose
AutoID	int	Identify unique values for this table.
AutoGUID	uniqueidentifier	Unique global identifier for this record.
ServerID	nvarchar(16) required default=ePO_SERVERNAME	Specifies the server for which this event is stored. The default value of this is the name of the ePO server and is installed as a default-constraint during installation of the ePO product software using the installer's token substitution.
AgentGUID	uniqueidentifier required	The reporting CMA agent identifier. Unique among all ePO agents on all ePO servers.
ReceivedUTC	datetime required default=GETDATE()	Date/time the event was stored into the database. Stored in UTC datetime format.
DetectedUTC	datetime required	Date/time when the analyzer detected this event. Different, and always prior to, the ReceivedUTC. See above. Stored in UTC format.
Analyzer	nvarchar(16) required	The software/hardware generating this event. This is analogous to the ePO traditional SoftwareID, or ProductCode. For example, VSE8000.
AnalyzerName	nvarchar(64) required	The product name as a displayable string
AnalyzerVersion	nvarchar(20) required	Version string of the analyzer.
AnalyzerHostName	nvarchar(128) optional	Network host name of the machine, including domain prefix as needed.
AnalyzerIPV4	int optional default=null	The 32-bit IPv4 address of the analyzer.
AnalyzerIPV6	binary(16) optional default=null	The 128-bit IPv6 address of the analyzer.
AnalyzerMAC	nvarchar(16) optional default=null	The MAC address of the analyzer.
AnalyzerDATVersion	nvarchar(20) optional default=null	If the threat was detected with a product which uses DAT technology and the event reports the detecting DAT version, it is stored here.
AnalyzerENGVersion	varchar(20) optional default=null	If the threat was detected with a product which uses scanning engine technology and the event reports the engine version string, it is stored here.
SourceHostName	nvarchar(128) optional	The threat source host name where applicable (such as IPS events if detectable).

Field	Attributes	Purpose
	default=null	
SourceHostName	nvarchar(128) optional default=null	The threat source host name where applicable (such as IPS events if detectable).
SourceIPV4	int optional default=null	The threat source 32-bit IPv4 address.
SourceIPV6	binary(16) optional default=null	The 128-bit IPv6 address.
SourceMAC	nvarchar(16) optional default=null	The threat source MAC address where applicable.
SourceUserName	nvarchar(128) optional default=null	The threat source user name or email address.
SourceProcessName	nvarchar(128) optional default=null	The threat source process name if detectable.
SourceURL	nvarchar(256) optional default=null	The threat source URL if detectable (for http requests that trigger threat detections).
TargetHostName	nvarchar(128) optional default=null	The threat target host name where applicable (such as IPS events if detectable).
TargetIPV4	int optional default=null	The 32-bit threat target IPv4 address.
TargetIPV6	binary(16) optional default=null	The 128-bit IPv6 address.
TargetMAC	nvarchar(16) optional default=null	The threat target MAC address where applicable.
TargetUserName	nvarchar(128) optional default=null	The threat target user name or email address.
TargetPort	smallint optional	The threat target port for network-homed threat classes.

Field	Attributes	Purpose
	default=null	
TargetProtocol	nvarchar(16) optional default=null	The threat target protocol for network-homed threat classes (HTTP, FTP, NETBIOS, SMTP, SNMP, select the protocol from your Linux /etc/services file).
TargetProcessName	nvarchar(128) optional default=null	The threat target process name where applicable.
TargetFileName	nvarchar(266) optional default=null	The threat target filename where applicable.
ThreatCategory	nvarchar(128) required	Hierarchical category string describing the threat. More information on the format of this string and valid values can be found here: EventCategories
ThreatEventID	uint32 required	Event ID (currently the TVD event identifier)
ThreatSeverity	uint32 required default=1	Severity of the event instance as a number ranging from one (1) through seven (7) with (1) being highest severity, (7) being lowest/informational.
ThreatName	nvarchar(128) required	Name of this threat, such as a virus, a firewall rule name, etc.
ThreatType	nvarchar(32) required	Analyzer-dependent classification of the internal event type. E.g. VirusScan stores this as "virus", "trojan", "pup, etc.
ThreatActionTaken	nvarchar(32) required default=none	Action taken against the threat, if any. E.g. cleaned, deleted, blocked, etc.
ThreatHandled	bit optional default=null	Indicates whether the threat was handled or not. Currently zero or one is supported, indicating not-handled and handled states. If the event is not threat oriented, set to null.